J. Austral. Math. Soc. 22 (Series A) (1976), 182–187.

A CONSTRUCTION FOR CERTAIN CLASSES OF SUPPLEMENTARY DIFFERENCE SETS

JOAN COOPER

(Received 1 December 1974)

Abstract

Let $v = ef + 1$ be a prime power, and consider G the cyclic group of order $v - 1$ with e cosets C_i of order f defined as $C_i = \{x^{ej+i} : 0 \leqq j \leqq f - 1\}$ and $0 \leqq i \leqq e - 1$, where x is a primitive element of $GF(p^\alpha)$ and a generator of G. By using these cosets we give a simple construction for certain classes of Supplementary Difference Sets, Difference Sets, and Szekeres Difference Sets. These classes are not new, but the simple method of construction is original.

By using cosets of the cyclic group G of order $v - 1$ (v a prime power) we give a simple construction for the following classes of Supplementary Difference Sets, Difference Sets, and Szekeres Difference Sets.

Supplementary Difference Sets

$$e - \{v; f; f - 1\} \qquad v = ef + 1;$$

$$e - \{v; f + 1; f + 1\} \quad v = ef + 1;$$

$$\frac{e}{2} - \left\{v; f; \frac{f-1}{2}\right\} \qquad v = ef + 1, f \text{ odd};$$

$$\frac{e}{2} - \left\{v; f + 1; \frac{f+1}{2}\right\} \quad v = ef + 1, f \text{ odd}.$$

Difference Sets

$$\left(v, f, \frac{f-1}{2}\right) \qquad v = 2f + 1, f \text{ odd};$$

$$\left(v, f + 1, \frac{f+1}{2}\right) \quad v = 2f + 1, f \text{ odd}.$$

Szekeres Difference Sets

$$2-\left\{v;f;\frac{f-1}{2}\right\}v=2f+1, f \text{ odd}.$$

These classes are not new (see Sprott, (1956)), however, the simple method of construction is original.

A set of k residues $D=\{a_1, a_2, \cdots, a_k\}$ modulo v is called a (v, k, λ)-difference set if among the collection of elements $[a_i\text{-}a_j\colon i\neq j,\ 1\leqq i, j\leqq k]$ each of the non-zero residues occurs precisely λ times.

Let $S_1, S_2, \cdots, S_n$ be subsets of V, an additive abelian group, containing $k_1, k_2, \cdots, k_n$ elements respectively. Write T_i for the totality of all differences between elements of S_i (with repetitions) and T for the totality of elements of all the T_i. If T contains each non-zero element a fixed number of times, λ say, then the sets $S_1, S_2, \cdots, S_n$ will be called $n-\{v; k_1, k_2, \cdots, k_n; \lambda\}$ supplementary difference sets, where v is the order of V.

$2-\{2m+1; m; m-1\}$ supplementary difference sets M and $N\in G$, an additive abelian group, are called Szekeres difference sets if $a\in M \Rightarrow -a\notin M$.

We will be using the parameter $v=ef+1=p^\alpha$ (a prime power) and the associated cyclic group G, of order $v-1$, which is the multiplicative group of the field $GF(p^\alpha)$. The cosets of G will be defined as

$$C_i=\{x^{ej+i}: 0\leqq j\leqq f-1\} \qquad 0\leqq i\leqq e-1,$$

where x is a primitive element of $GF(p^\alpha)$ and a generator of G.

The basic concepts of group theory and linear algebra have been assumed. For any reference to group theory see M. Hall Jr. (1959).

We shall be concerned with collections in which repeated elements are counted multiply rather than with sets. If T_1 and T_2 are two collections (or sets), then $T_1 \& T_2$ will denote the adjunction of T_1 to T_2 with total multiplicities retained. We will use square brackets [ ] to denote collections and braces { } to denote sets.

EXAMPLE. Let $S_1=\{1,2,x+1,2x+2\}$, $S_2=\{0,1,2,x+1,2x+2\}$ be two sets. Then

$$S_1 \& S_2=[0,1,1,2,2,x+1,2x+2,2x+2].$$

The class product of two collections (or sets) T_1 and T_2 will be denoted by $T_1\wedge T_2$ which is defined as

$$T_1\wedge T_2=[x_1+x_2: x_1\in T_1, x_2\in T_2].$$

The transpose of a coset, C_i^T, will be defined as $-C_i$ where

$$\begin{aligned}-C&=-\{x^{ej+i}: 0\leqq j\leqq f-1\}\\ &=\{-x^{ej+i}: 0\leqq j\leqq f-1\}.\end{aligned}$$

In Storer (1967) p. 24 it is shown that

$$-1 = x^{eq+k} \text{ where } 0 \leqq q \leqq k-1$$

(1)

$$\text{and } k = \begin{cases} \frac{e}{2} & f \text{ odd} \\ 0 & f \text{ even} \end{cases}$$

Thus

$$C_i^T = \{x^{e(q+j)+i+k} : 0 \leqq j \leqq f-1\}.$$

For proofs of the following four lemmas see Cooper (1972).

LEMMA. 1. *If C_i is a coset of the cyclic group G then*

$$C_i \wedge C_i^T = [x^{ej+i} + x^{e(q+t)+i+k} : 0 \leqq j, t \leqq f-1]$$

$$= f\{0\} \mathbin{\&} \mathop{\&}_{s=0}^{e-1} a_s C_s \quad a_s \text{ are integer}$$

and

$$\sum_{s=0}^{e-1} a_s = f-1.$$

LEMMA 2. *If C_i and C_j are cosets of the cyclic group G then*

$$C_i \wedge C_j = \mathop{\&}_{s=0}^{e-1} a_s C_s \qquad (C_j \neq C_i^T)$$

and

$$\sum_{s=0}^{e-1} a_s = f.$$

LEMMA 3. *If* $C_i \wedge C_j = \mathop{\&}_{s=0}^{e-1} a_s C_s$

then $$C_{i+1} \wedge C_{j+1} = \mathop{\&}_{s=0}^{e-1} a_{s+1} C_s.$$

LEMMA 4. *If C_i is a coset of G then*

(*i*) $C_i^T = C_i$ *if f is even*

(*ii*) $C_i^T = C_{i+\frac{e}{2}}$ *if f is odd.*

https://doi.org/10.1017/S1446788700015305 Published online by Cambridge University Press

[Note: $\overset{e-1}{\underset{s=0}{\&}} C_s = G$.]

We will start by considering the collection of differences between the elements of C_i. This collection is given by

$$(2) \qquad [x^{ej+i} - x^{et+i} : 0 \leqq j, t \leqq f-1,\ j \neq t]$$

$$= [x^{ej+i} + (-1)x^{et+i} : 0 \leqq j, t \leqq f-1, j \neq t]$$

$$= [x^{ej+i} + x^{eq+k}(x^{et+i}) : 0 \leqq j, t \leqq f-1, j \neq t] \text{ (from (1))}$$

$$(3) \qquad = [x^{ej+i} + x^{e(q+t)+k+i} : 0 \leqq j, t \leqq f-1, j \neq t].$$

Now equation (3) corresponds to $C_i \wedge C_i^T$ (see lemma 1) with the terms that add to zero excluded. Thus the collection of differences between the elements of any coset C_i will be given by

$$\overset{e-1}{\underset{s=0}{\&}} a_s C_s \qquad \left(\text{where } \sum_{s=0}^{e-1} a_s = f-1\right)$$

(see Lemma 1).

We will talk about the collection of differences between elements of any coset C_i in terms of

$$C_i \wedge C_i^T = \overset{e-1}{\underset{s=0}{\&}} a_s C_s \text{ (terms adding to zero excluded).}$$

THEOREM 5. *Let $v = ef + 1 = p^\alpha$ (a prime power) and G the associated cyclic group of order $v-1$. The set of e-disjoint cosets from the cyclic group G form*

$$e - \{v; f; f-1\} \textit{ supplementary difference sets.}$$

PROOF. The collection of differences from any coset is given by

$$C_i \wedge C_i^T = \overset{e-1}{\underset{s=0}{\&}} a_s C_s \text{ (terms adding to zero excluded).}$$

Now the totality of differences from all cosets will be

$$\overset{e-1}{\underset{l=0}{\&}} C_{i+l} \wedge C_{i+l}^T = \overset{e-1}{\underset{l=0}{\&}} \left(\overset{e-1}{\underset{s=0}{\&}} a_s C_{s+l} \right) \text{ (see Lemma 3)}$$

$$= \overset{e-1}{\underset{s=0}{\&}} a_s \left(\overset{e-1}{\underset{l=0}{\&}} C_{s+l} \right)$$

$$= \overset{e-1}{\underset{s=0}{\&}} a_s G$$

$$= (f-1)G \text{ (see Lemma 1).}$$

https://doi.org/10.1017/S1446788700015305 Published online by Cambridge University Press

Thus in the totality of differences from the cosets every non-zero elements occur $(f-1)$ times and the e cosets C_i of order f form

$$e-\{v;f;f-1\} \text{ supplementary difference sets.}$$

LEMMA. 6. *If f is odd the first $\frac{1}{2}e$ cosets $C_0, C_1, \cdots, C_{\frac{1}{2}e-1}$ form*

$$\frac{e}{2}-\left\{v;f;\frac{f-1}{2}\right\} \textit{ supplementary difference sets.}$$

PROOF. From the definition of C_i^T the collection of differences from C_i^T will be the same as that of C_i.

If f is odd $C_i^T = C_{i+\frac{e}{2}}$ (Lemma 4) and

$$\mathop{\&}_{l=0}^{\frac{e}{2}-1} C_{i+l} \wedge C_{i+l}^T = \mathop{\&}_{s=\frac{e}{2}}^{e-1} C_{i+l} \wedge C_{i+l}^T.$$

From Theorem 5, $\mathop{\&}\limits_{l=0}^{e-1} C_{i+l} \wedge C_{i+l}^T = (f-1)G$; thus for f odd

$$\mathop{\&}_{l=0}^{\frac{e}{2}-1} C_{i+l} \wedge C_{i+l}^T = \frac{f-1}{2}G.$$

LEMMA 7. *If $v = 2f+1$ and f is odd, then C_0 and C_1 form*

(*a*) $\left(v, f, \dfrac{f-1}{2}\right)$ *difference sets, and*

(*b*) $2-\{v;f;f-1\}$ *Szekeres difference sets.*

PROOF. (a) Immediate from Lemma 6.

(b) As f is odd, $C_i^T = C_{i+\frac{e}{2}}$ and $C_0^T = C_1$.

Now if $a \in C_0$, $-a \in C_1$, from the definition of Szekeres difference sets, C_0 and C_1 form

$$2-\{v;f;f-1\} \text{ Szekeres difference sets.}$$

THEOREM 8. *Let $v = ef+1 = p^\alpha$ (a prime power) and G the associated cyclic group of order $v-1$. The e-sets $\{0\} \cup C_i$,*

$i = 0, 1, \cdots, e-1$, where C_i are the cosets of G_i, form

$$e-\{ef+1;f+1;f+1\} \textit{ supplementary difference sets.}$$

PROOF. From Theorem 5 the collection of differences for any coset is expressed as

$$\mathop{\&}_{s=0}^{e-1} a_s C_s.$$

https://doi.org/10.1017/S1446788700015305 Published online by Cambridge University Press

It can easily be seen that the differences between the elements of C_i and $\{0\}$ will give C_i and $-C_i = C_i^T$.

Thus the collection of differences of $\{0\} \cup C_i$ will be given by

$$\mathop{\&}_{s=0}^{e-1} a_s C_s \& C_i \& C_i^T.$$

Now the totality of differences from the set of cosets will be

$$\mathop{\&}_{l=0}^{e-1} \left(\mathop{\&}_{s=0}^{e-1} a_s C_{s+l} \& C_{i+l} \& C_{i+l}^T \right)$$

$$= (f-1)G \& G \& G = (f+1)G.$$

As every non-zero element occurs $(f+1)$ times, we have

$$e - \{v; f+1; f+1\} \text{ supplementary difference sets.}$$

LEMMA 9. *Let $v = ef + 1$ and f odd, then the sets $\{0\} \cup C_i$, $i = 0, 1, \cdots, \frac{e}{2} - 1$ form*

$$\tfrac{1}{2}e - \left\{ ef + 1; f + 1; \frac{f+1}{2} \right\} \textit{ supplementary difference sets.}$$

The proof is similar to that for Lemma 6 and Theorem 8.

LEMMA 10. *If $v = 2f + 1$ and f is odd then $\{0\} \cup C_0$ and $\{0\} \cup C_1$ form $\{v; f+1; (f+1)/(2)\}$ difference sets.*

The proof follows from Lemma 9.

Bibliography

Joan Cooper and Jennifer Wallis (1972), 'A construction for Hadamard arrays', *Bull. Austral. Math. Soc.* 7, 269–278.

Joan Cooper (1972), 'A binary composition for collections and sets', (Proceedings of the *First Australian Conference on Combinatorial Mathematics*, edited by J. and W. Wallis, T.U.N.R.A., 145–161, Newcastle, N.S.W., 1972).

Marshall Hall Jr. (1959), *Theory of Groups*, (MacMillan, New York, 1959).

D. A. Sprott (1956), 'Some series of balanced incomplete block designs', *Sankhya* Ser. A17, 185–192.

J. Storer (1967), *Cyclotomy and Difference Sets*, (Lectures in Advanced Mathematics, 2, Markham, Chicago, Illinois, 1967).

Jennifer Wallis (1972), 'On supplementary difference sets', *Aequations Mathematicae*, **8**, 242–257.

W. D. Wallis, Anne Penfold Street, Jennifer Seberry Wallis (1972), *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*, (Lecture Notes in Mathematics, Vol. 292, Springer-Verlag, Berlin-Heidelberg-New York, 1972).

Mathematics Department
University of Newcastle
Newcastle, N.S.W. 2308
Australia.